Data Protection and Information Security Frequently Asked Questions

The purpose of this document is to outline data protection and information security details of Incision services.

With this document, Incision intends to create a common list of answers to typical questions made by Privacy Managers, DPOs, IT Managers, etc. to assess the compliance of Incision services with the relevant data protection and information security legislations and standards.

This document, redacted by internal Privacy & Security resources of Incision and approved by its Management, is aimed by the will to approach business in total transparency and accountability.

The content of this document is related to the date of its approval indicated below and it will be reviewed and updated regularly.

If you have any question about the content of this document, please contact your commercial reference at Incision or write to privacy.security@incision.care.

---

1. **Do Incision services comply with the General Data Protection Regulation** (Regulation EU 679/2016, also known as "GDPR")**?** → **YES**. Incision human resources work jointly and on a daily basis to comply, and maintain compliance, with the GDPR.
2. **Does Incision follow the security requirements of HIPAA** (Health Insurance Portability and Accountability Act)**?** → **YES**. Even if Incision services do not process, and are not meant to process, any health information on behalf of the Customer, Incision decided to take the security requirements of HIPAA as a standard for its security framework.
3. **Does Incision process special categories of personal data to provide its services?** → **NO**. Incision doesn't process special categories of personal data (art. 9, paragraph 1, of GDPR), like medical information, thorough its services.
4. **Do Incision services comply with other relevant data protection legislations?** → **YES**. Incision offer its services on an international scale and, as consequence, needs to comply with many other State laws (for instance: the Dutch General Data Protection Regulation Implementing Act, the UK GDPR and Data Protection Act, Egyptian Law on the Protection of Personal Data, etc.).
5. **Does the Medical Device Regulation apply to Incision services?** → **NO**. Incision services are not considered medical devices or accessories for such devices. Our purpose is to provide high quality training and organizational tools for OR specialists (or future specialists). For this reason, Incision does not, and doesn't need to, process health information thorough its services.
6. **Is Incision certified ISO/IEC 27001?** → **In the foreseeable future**. Incision is currently assessing ISO/IEC 27001 compliance requirements and intends to get certified in the foreseeable future.
7. **What is the relation between Incision and the Customer regarding the processing of personal data?** → **Incision is the processor of the Customer, which is the controller**. To provide its services, Incision needs to process personal information on behalf of the Customer (depending on the nature of the Customer and the service provided: OR personnel data, students data, etc.).
8. **Does Incision use external providers to provide its services?** → **YES**. Incision, to ensure a high level of quality, security and availability of its services, uses the following external providers (each of them signed with Incision a specific Data Processing Agreement that appoints them as sub-processors):

Provider	Purpose	Storage location	Certifications
Amazon Web Services ("AWS")	Storage of all data processed by Incision services	AWS Region (Ireland)	ISO/IEC 27001 ISO/IEC 27701
Levi9	Product maintenance	Levi9 only access, when needed, personal data without storing it	ISO/IEC 27001

9. **Are Incision services performed under certain contractual standards of data protection?** → **YES**. Incision performs the processing activities on behalf of the Customer under the general application of the Data Protection Agreement available on https://www.incision.care/terms-and-conditions. Out of signing Incision Business Terms and Conditions, no further agreement is necessary between Incision and the

Customer. On Incision website are also available Incision's processor obligations, a tool to have a quick and clear overview of our responsibilities. Since Incision provides hundreds of customers, it needs to be bound to a standard DPA. In case the Customer needs to further instruct Incision about the processing of personal data, it shall contact its commercial reference at Incision or write to privacy.security@incision.care.

10. **Is Incision able to support the Customer with a data subject request? → YES**. Incision has the full control of the personal data processed for the purpose of providing its services and, as a result, is able to fully support the controller in any process made to honor a data subject request.
11. **Is Incision capable to be immediately aware of a personal data breach occurred on the personal data processed on behalf of the Customer? → YES**. AWS has an automated alert system that notify in real time both Incision and Levi9 of any event that, even potentially, can bring to a loss of integrity, availability or confidentiality of personal data. Incision successfully tested the efficiency of the alert system and the quick response of its teams.
12. **Does incision have a dedicated person to handle compliance with relevant data protection legislations? → YES**. Incision hired a full-time Privacy & Security Specialist which is fully dedicated to ensuring compliance with relevant data protection legislation and information security standards.
13. **Are personal data processed by Incision on behalf of the Customer encrypted? → YES**. On AWS Incision applies by default encryption at rest (AES-256). Incision applies the protocol https to communicate with AWS databases.
14. **Does Incision back-up all personal data processed on behalf of the Customer? → YES**. AWS regularly organize back-up of all personal data and keeps them separated from the originals, applying the same level of security.
15. **Is Incision able to limit the access to personal data processed on behalf of the Customer? → YES**. Incision employees access to personal data processed to provide its services on a least privilege, access limitation, and need to know base. All Incision employees received specific training regarding data protection and information security.

Date of approval: 28/10/2022